名古屋港コンテナターミナルのシステム障害を受けた対応

国土交通省

資料２

○ 令和5年7月、名古屋港コンテナターミナルのシステムがランサムウェアに感染し、約3日間にわたりコンテナの搬入・搬出作業が停止
○ 同7月、有識者等からなる「コンテナターミナルにおける情報セキュリティ対策等検討委員会」を設置
○ **緊急的対策**として、専門家の知見を踏まえた港湾分野における情報セキュリティ対策を事業者に周知徹底
○ 情報セキュリティ対策等の推進のための**制度的措置**についても同委員会で検討

システム障害の概要

○対象：名古屋港統一ターミナルシステム(NUTS)※

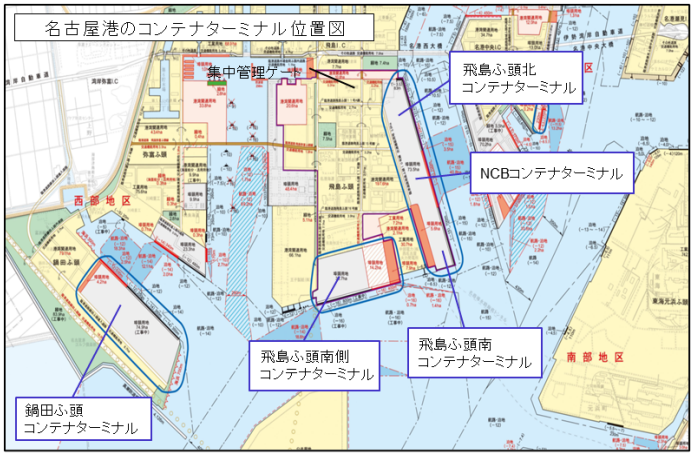
※名古屋港の5つのコンテナターミナルにおけるコンテナの積みおろし作業、搬入・搬出等を一元的に管理するシステム

○原因：不正プログラム（ランサムウェア）への感染

○影響：令和5年7月4日から7月6日までの3日間において、

・荷役スケジュールに影響が生じた船舶 37隻

・搬入・搬出に影響があったコンテナ 約2万本（推計）



有識者委員会における検討等

第1回 令和5年 7月31日	名古屋港の事案の原因及び対応策の分析 システムを運用する名古屋港運協会等からのヒアリング
第2回 9月29日	**中間取りまとめ①　【緊急的対策】** （情報セキュリティ対策、システム障害発生時の対応策） ・10月2日、関係事業者に周知、必要な措置を講じるよう注意喚起 ・11月～12月、全国4か所（東京、名古屋、大阪、福岡）で説明会を実施
第3回 11月30日	**中間取りまとめ②　【制度的措置】** （サイバーセキュリティ政策及び経済安全保障政策における港湾の位置付け）
第4回 令和6年 1月24日	**取りまとめ** **○港湾運送事業法の観点** 一般港湾運送事業者が作成する事業計画にターミナルオペレーションシステムの概要や情報セキュリティの確保に関する事項の記載を求め、**国が審査する仕組みを導入** **○サイバーセキュリティ基本法の観点** 「重要インフラのサイバーセキュリティにかかる行動計画」を改定し、**重要インフラ分野に「港湾分野」を位置付ける**方向で検討 **○経済安全保障の観点** 経済安全保障の観点からも国として積極的な関与を行うため、経済安全保障推進法の趣旨も踏まえ、ターミナルオペレーションシステム（TOS）を使用して役務の提供を行う**一般港湾運送事業を経済安全保障推進法の対象事業とすることが必要**であると考えられる。